Statement by

Scott Charbo

Chief Information Officer

Department of Homeland Security

Before the

House Government Reform Committee

Hearing on

Information Security and

Implementation of the Federal Information Security Management Act of 2002

March 16, 2006

Thank you Mr. Chairman and Members of the Subcommittee for allowing me this opportunity to testify before the House Committee on Government Reform on the subject of Information Security and the Department of Homeland Security's implementation of the Federal Information Security Management Act (FISMA) of 2002. My prepared remarks will cover the status of the Department's implementation of FISMA.

The mission of the Department of Homeland Security's Information Security Program is to provide the Department with a secure and trusted computing environment that enables the Department to leverage Information Technology (IT) and effectively and securely share information in support of its many and varied missions. To this end, statutory compliance is a top priority, and the Department's Information Security Program is structured around compliance with the Federal Information Security Management Act (FISMA), as well as Office of Management and Budget, and National Institute of Standards and Technology guidance.

The Department's Program has come a long way in just three short years. In 2003 and 2004, the Department laid a necessary foundation of effective security policies and architecture guidance. Policies are now codified in a dedicated Management Directive and the systems security architecture is fully integrated into the Department's Enterprise Architecture. Security policies and systems security architecture are both updated on a regular basis, and compliance is enforced through the use of several mandatory security management tools that are now in use throughout the Department. These early program-development steps have given the Department an important foundation, and building on those early efforts, the Department completed three major information security initiatives in 2005.

First, a comprehensive systems and applications inventory was completed in August 2005. The Department-wide FISMA inventory is based on a detailed methodology for identifying systems and applications using standard federal definitions. This inventory now provides clear accreditation boundaries for each and every operational IT system supporting the Department’s diverse missions and assigns responsibility for security controls to specific individuals, thereby providing a baseline for measuring security compliance. To ensure the inventory remains accurate, annual inventory reviews will continue each year with a near term focus in 2006 of linking the inventory to the Department’s capital planning and investment control processes, allowing the Department to better integrate effective security controls at the beginning of the systems' life-cycle. In the Department's fiscal year 2005 FISMA report, the Inspector General acknowledged for the first time the completeness and accuracy of our FISMA inventory.

Second, an enterprise certification and accreditation tool was successfully fielded in April 2005, and that is now fully integrated with a FISMA management tool fielded in 2004. These tools automate many of the day-to-day security tasks associated with FISMA compliance, thereby easing the security burden on system owners. The result is a consistent and cost-effective set of security management procedures in use throughout the Department.

Third, a comprehensive and repeatable set of information security metrics significantly improved system owner accountability. These metrics now measure and inform progress in completing the accreditation of all operational systems, as well as other key compliance activities throughout the Department. Monthly information security scorecards provide detailed status updates to Department leadership, and these scorecards are proving highly successful for improving the accountability of system owners.

These three initiatives build on earlier milestones and have now paved the way for real and measurable cyber security improvements in the near future. With momentum from these initial successes, the Department implemented an aggressive Remediation Project for 2006, with a goal of 100% remediation by the end of the year. Originally announced by Secretary Chertoff in his keynote address at the Department's annual Security

Conference last August, the Project moved into full swing in October 2005, and the Department is well on its way to full remediation.

The Department's FISMA inventory currently includes approximately 700 systems, and prior to the initiation of the Remediation Project, the number of fully accredited systems was only 26% Department-wide. By the end of February of this year, over 60% of the systems are fully accredited. In just 5 short months the Department has more than doubled the number of accredited systems, and it is on track to make the goal of full remediation by the end of this year. It is clear the Project is positively affecting the security culture of the Department, and recent upward trends in remediation metrics support that view.

Until now, I have only addressed Program-specific, systems-and-applications security compliance initiatives. However, the Department must also ensure those systems and applications are connected across a secure enterprise backbone providing common shared IT services. To accomplish this goal an aggressive Infrastructure Transformation Program called "OneNet" was initiated for 2006, to bring all legacy information technology infrastructures under a single enterprise program. Benefits of this approach are many, to include network optimization and improved quality-of-service, both of which will significantly enhance information sharing initiatives. The enterprise will operate at considerably lower life-cycle costs in the future.

Planning for “OneNet” began with a comprehensive security framework that is consistent with the detailed systems security architecture of the Department. The Department's security framework provides systems owners with common, shared enterprise IT services, where information at differing sensitivities and users at differing levels of trust have assured information sharing through the use of Security Trust Domains. This framework now provides a strong security foundation from which to build upon in the future, and enhanced security represents the single biggest benefit from the OneNet Project.

As part of the "OneNet" effort, the Department is also fielding its first enterprise-wide network operations and security center. The center is responsible for managing the Department's shared IT enterprise environment in real-time, including the discovery and remediation of security incidents as they occur, and represents a significant improvement to our overall security posture.

I am confident that the DHS Information Security Program is moving in the right direction and I look forward to working with you and your staff in the future, as, together, we "secure the success of DHS."

Thank you and I look forward to your questions.